Section II: **Administrative Security**
Title: **Information Security Risk Management Standard**
Current Effective Date: **June 30, 2008**
Revision History: **June 12, 2008**
Original Effective Date: **June 30, 2008**

Purpose: To ensure that the North Carolina (NC) Department of Health and Human Services (DHHS) Divisions and Offices properly identify potential problems before they occur so that risk-handling activities may be planned and invoked as needed to mitigate adverse impacts.

STANDARD

1.0 Background

The Divisions and Offices management, with the assistance from the Division Information Security Official (ISO), shall ensure that risks are identified, analyzed, and documented periodically in order to evaluate the effectiveness of existing key risk controls, as deemed necessary. In addition, Divisions and Offices must establish their own policies, procedures, standards, and guidelines for the mitigation and handling of risk.

2.0 Key Risk Factors

Key risks must be identified to ensure a defined line of business is safeguarded against any type of potential exposure. This standard will only illustrate three (3) types of key risk factors that may exist at the Divisions and Offices; however, the state-wide network security posture may not be limited to these key risk factors:

- *Business Risk*: The cost and/or lost revenue associated with an interruption of normal business operations.
- *Organizational Risk*: Loss associated directly or indirectly with the following:
  - Inadequate or failed internal process
  - People
  - Systems
  - External events
- *Information Technology Risk*: The loss of an automated system, network, or other critical information technology resource that would adversely affect a line of business.

3.0 Pre-Risk Assumptions

All Divisions and Offices management, with assistance from the Division ISO, are responsible for determining who will participate in the pre-risk assumptions. The assigned workforce members who will participate in the pre-risk assumptions must complete the ITS – Enterprise Security and Risk Management Office, Risk Management Services.

The assigned DHHS workforce members' roles and responsibilities for the pre-risk assumptions must include reading and understanding the Division and Office mission statement in conjunction with understanding how information technology (IT) affects the mission of the particular Division and Office.

DHHS workforce members responsible for completing the pre-risk assumptions shall ensure the following:

- The line of business should be identified and clearly defined.
- The defined line of business must identify all critical information resources.
- The information resources identified must assist in supporting the defined line of business.
- A Data Steward for each line of business must be identified. For additional information, refer to the NC DHHS Security Standards, Administrative Security Standards – Data Stewardship Security Standard.
- A DHHS workforce member must be identified to implement the processes outlined in the Risk Management Guide. For additional information, refer to Section 5.0: Conducting the Risk Assessment Process, listed below.
- The legal parameters that control the delivery of a defined line of business must be clearly understood and documented.

Once the pre-risk assumption is completed, the Division ISO must ensure that the results are recorded and filed in a secure location.

4.0 Conducting the Risk Assessment Process

The Divisions and Offices management shall choose the assigned workforce member, with the assistance from the Division ISO, to be responsible for participating and conducting the risk assessment process.

The risk assessment process presented in this section illustrates a three (3) phase approach for Divisions and Offices to follow, as identified below:

- *Phase I (Identify):* Phase I begins with the assigned workforce members identifying key risks utilizing a questionnaire (i.e., ITS – Risk Assessment Questionnaire). The questionnaire will be utilized to evaluate threats, liabilities, and vulnerabilities both known and potential, which may adversely impact a particular line of business. Phase I risks that are rated as *low* would require a lower level of security and/or business continuity planning. Risks rated as *moderate* or *high* proceed to Phase II (Analyze).
- *Phase II (Analyze):* Phase II begins with the assigned workforce members further analyzing the risks identified in Phase I by completing the more detailed remainder of the questionnaire discussed above. The risks rated as *low* in Phase II will be managed in a similar fashion as those rated *low* in Phase I. Risks rated as *moderate* or *high* will proceed to Phase III (Manage).
- *Phase III (Manage):* Phase III begins with the Division and Office management, who must obtain assistance from the assigned workforce members to further analyze the different effects and methods required for reducing risk. A documented action plan must be created and followed to detail, mitigate, or remove any risk. The results of the documented action plan must be used to

secure and safeguard DHHS data and information. Phase III risks necessitate a *high* level of security and/or business continuity planning.

The Phase I – Risk Assessment Questionnaire will document the results of the risk assessment process by the following three (3) levels of risk rating:

- *Low:* An event that could be expected to have a limited adverse effect on Division and/or Office operations (e.g., including missions, functions, images, and assets) and could cause limited degradation in mission capability. This would result in minor corrective actions or repairs.
- *Moderate:* An event that could be expected to have a serious adverse effect on Division and/or Office operations causing significant degradation in mission capability. A moderate event would place the Division and/or Office at a significant disadvantage resulting in major damage or loss to assets and would require extensive corrective actions or repairs.
- *High:* An event that could be expected to have a severe or catastrophic adverse effect on the Division and Office operations, which could cause a loss of mission capability for a period that poses a threat to human life or results in a loss of major assets.

The Phase I – Risk Assessment Questionnaire will analyze the risk impact categories relative to the risk level ratings given above. The risk impact categories shall include, but may not be limited to the following:

- *Operations:* Functions that support delivery of Division and Office business services (e.g., space allocation [facilities/campus/building], workforce, purchasing, financial, communications, etc.)
- *Technology:* Information assets that support the information technology (IT) infrastructure (e.g., security, hardware, software, middleware, network, communication systems, etc.)
- *Legal:* Parameters established by legislative mandates, federal/state laws, regulatory regulations, general statutes, policies, procedures, standards, guidelines, directives, and executive orders that impact delivery of program services
- *Citizen Services:* Program services mandated by charters, legislations, laws, regulations, general statutes, policies, procedures, standards, or guidelines that provide for the delivery of the state's business operations (e.g., education services, human services, highways, law enforcements, health/safety services, unemployment benefits, vital records, etc.)
- *Reputation:* General estimation by the public on how the state service is delivered (e.g., integrity, credibility, trusts, customer satisfactions, images, media relations, political involvements, etc.)

Once each phase of the risk assessment process has been documented, the Division ISO shall ensure that the results are recorded and filed in a secured location against any type of tampering or malice.

4.1 Phase I – Identify Risks

By completing the ITS, Phase I – Risk Assessment Questionnaire, the Divisions and Offices will be responsible for identifying, analyzing, managing, and documenting the following:

1. A list that includes the purpose of the mission critical information resources in conjunction with the following categories:

- Present information resource security and access controls and the techniques necessary to evaluate the controls
    - For additional information, refer to the NC DHHS Security Standards, Physical Security Standards – Physical Access Control Security Standard, Site Security Plan Standard, and the Perimeter Security Standard for assistance in security and access control information
- Information classification of the data and/or information stored or supported on a critical information resource, the data and/or information must be analyzed to evaluate the potential impact of harm that the loss of confidentiality, integrity, or availability would have on information technology (IT) assets and business operations
    - For additional information, refer to the NC DHHS Security Standards, Administrative Security Standards – Information Classification Security Standard for assistance in classifying data and/or information

2. The possibility of threats to the defined lines of business and to the information resources that support the lines of business. These types of possible threats can include but are not limited to the following types:

    - *Natural*: May include floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other events.
    - *Human*: May include events either enabled by or caused by human beings such as unintentional acts (inadvertent data entry) or deliberate actions (e.g., network based attacks, malicious software uploads, unauthorized access to confidential information, etc.).
    - *Environmental*: May include long-term power failures, pollutions, chemicals, and liquid leakages.

3. The vulnerabilities where threats could likely attack and cause business failure are defined in the NC DHHS Security Standards, Network Security Standards – Network Architecture Security Standard.

4. The probability of a threat occurring to the defined line of business. The likelihood that a threat could occur shall be described by using a *Low*, *Medium*, and *High* ranking scale:

    - *Low:* A *low* threat lacks sufficient capability or controls are in place to prevent the vulnerability from being exercised.
    - *Medium:* A *medium* threat is sufficiently capable but controls are in place that may impede successful exploitation of the vulnerability.
    - *High:* A *high* threat is sufficiently capable of occurring and existing controls to prevent the vulnerability from being exploitive are ineffective.

Once Phase I of the Risk Assessment Questionnaire has been documented, the results must be ranked. For more information regarding the ranking of results, refer to ITS – Phase I – Scoring Weight of the Risk Assessment Questionnaire. The following ranking scale must be used:

- *Low* will mean that a lower level of security and/or business continuity exists. This will end the assessment process.
- *Moderate* or *High* will proceed to Phase II – Analyze Risks, for additional analysis.

The Division and Office management and the Divisions ISO, based on current policies, procedures, and standards, may assign a workforce member to use a threat modeling approach to identify threats, if applicable.

The DHHS assigned workforce members shall identify threats to the information resources that support the defined line of business. The DHHS assigned workforce members responsible for identifying threats must then understand the threats by walking through potential threat scenarios that could occur. The DHHS assigned workforce member must categorize threats based on the incident types listed in the NC DHHS Policy and Procedure Manual, Section VII – Security and Privacy, Security Manual, Information Incident Management Policy.

The DHHS assigned workforce members shall identify mitigation strategies to see how potential threats could be mitigated. The mitigation strategies will vary depending on the Division or Office (it is out of the scope of this standard to provide specific mitigation strategies). The DHHS assigned workforce members must test the threat model by using the penetration testing results that are completed only by the DHHS Privacy and Security Office (PSO). The penetration testing investigates threats by directly assessing a system in an informed or uninformed manner.

4.2 Phase II – Analyze Risks

The DHHS assigned workforce members responsible for the ITS – Phase II – Risk Assessment Questionnaire shall perform the following:

- Must review the Phase I list of questions and documented results before they begin Phase II. Phase II questions are to be a further extension of questions raised in Phase I, but will require the Divisions and Offices to analyze risks should they occur to the defined line of business.
- Must have a general understanding of important Division and Office mission critical information resources to include, but not limited to the following:
  - Licensed program applications
  - Program application databases
  - Software (application and database) and hardware inventories
  - People that support the defined line of business

The results of, Phase II shall use the following scale:

- *Low* will result in cessation of the analysis with this phase (the assessment will not continue).
- *Moderate* or *High* are subject to a gap analysis and action plan in Section 4.3 below.

For additional information regarding the ranking scale used for Phase II, refer to the ITS, Phase II – Scoring Weight of the Risk Assessment Questionnaire.

4.3 Phase III – Risk Management

The DHHS assigned workforce members responsible for the ITS, Phase III – Risk Assessment Questionnaire shall perform the following:

- Must perform a gap analysis of the risks identified and documented in Phases I and I of the Risk Assessment Questionnaire by having the assigned workforce members analyze the necessary methods required for the reducing risks.
- Must provide mitigation planning by identifying how to perform the following:
  - How to avoid risks associated with the defined line of business,
  - How to acknowledge where risks cannot be cost effectively managed to the defined line of business,
  - How to reduce the impact of risks associated with the defined line of business,
  - How to transfer the risks associated with the line of business, and
  - How to limit probability of occurrence within the defined line of business.

The Division ISO shall ensure that a business analysis is performed and documented to include the following information:

- Cost implications of providing necessary controls to mitigate risk
- Benefits and costs of applying risk mitigation options/countermeasures (controls) individually or in combination
- Balance cost of implementing each mitigation option to benefits derived from the implementation of a proposed option

The Division ISO should file the results of the business analysis in a secure location in order to prevent tampering or any malicious acts. The Divisions and Offices management and the Division ISO must perform the following:

- Must select and implement risk mitigation controls that limit risk to a defined line of business.
- Must update the business continuity plan that documents the chosen risk mitigation controls that are to be implemented.

5.0 Post-Assessment Risk Guide

The Division and Office management and the Division ISO should select workforce members, preferably the workforce members that participated in the risk assessment process, to comply with the following:

- Compile and report the status of risks associated with the defined line of business and the mitigation plans to combat those risks.
- Analyze and record the changes in risks to the defined line of business over time. Changes must be made to the documentation filed by the Division ISO to ensure all documentation is correct.
- Take corrective actions as needed to improve risk management in the Division and Office.

Reference:

- NC Statewide Information Technology Services, Enterprise Security and Risk Management Office – Risk Management Services, Risk Management Guide

- NC Statewide Information Technology Services, Statewide Information Technology Policy – November 2004, Security Policy and Guidelines
    - Information Technology Risk Management Policy with Guidelines

- NC DHHS Security Standards
    - Administrative Security Standards
        - Data Stewardship Security Standard
        - Information Classification Security Standard
    - Network Security Standards
        - Network Architecture Security Standard
    - Physical Security Standards
        - Perimeter Security Standard
        - Physical Access Control Security Standard
        - Site Security Plan Standard

- NC DHHS Policy and Procedure Manual, Section VIII – Security and Privacy, Security Manual
    - Information Incident Management Policy
    - Risk Management Policy